



REPLY TO  
ATTENTION OF:

DEPARTMENT OF THE ARMY  
HEADQUARTERS, 41<sup>ST</sup> FIRES BRIGADE  
BUILDING 10053, BATTALION AVENUE  
FORT HOOD, TX 76544


AFYB-FB-CDR

8 December 2009

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Brigade Command Policy Letter # 10 – SIPR Port Security Violations

1. REFERENCE: AR 25-2, Information Assurance, 23 March 2009 and Network Enterprise Center (NEC) Policy #2009-07, Fort Hood Network Access Control Policy, 13 July 2009.
2. PURPOSE: To provide SIPR users with a clear understanding of the procedures and consequences for security violations while operating a computer on the classified network.
3. POLICY: Classified computers owned and operated by 41<sup>st</sup> Fires Brigade will follow the guidelines established by Network Enterprise Command. Classified/SIPR computers can only be connected to specific ports to which they have been assigned according to the approved Tenant Security Plan (TSP) dated 5 October 2009. All classified computers have been labeled with their assigned ports. It is the individual user's responsibility to ensure that classified/SIPR computers are not connected to any other port other than the one to which they have been assigned.
4. PROCEDURE: When a user connects a computer to the wrong port, it results automatically in a security violation. The NEC will immediately shut off that port. This violation will require a memorandum prepared by the BDE S6 and signed by the BDE Commander to reestablish connectivity to that port. The first violation will result in a formal counseling and retraining by Brigade Automations Officer. A second violation will result in the user's SIPR access being disabled and/or revoked.
5. The point contact for this memorandum is the Brigade S6 section at 254-288-6898 or 254-553-0238.

  
JOHN C. THOMSON III.  
COL, FA  
Commanding

DISTRIBUTION:

A